Experimental Demonstration of Counterfactual Quantum Communication

Yang Liu, Lei Ju, Xiao-Lei Liang, Shi-Biao Tang, Guo-Liang Shen Tu, Lei Zhou, Cheng-Zhi Peng, Kai Chen,* Teng-Yun Chen,† Zeng-Bing Chen, and Jian-Wei Pan

Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

(Received 24 August 2011; published 19 July 2012)

Quantum effects, besides offering substantial superiority in many tasks over classical methods, are also expected to provide interesting ways to establish secret keys between remote parties. A striking scheme called ''counterfactual quantum cryptography'' proposed by Noh [Phys. Rev. Lett. **103**, 230501 (2009).] allows one to maintain secure key distributions, in which particles carrying secret information are seemingly not being transmitted through quantum channels. We have experimentally demonstrated, for the first time, a faithful implementation for such a scheme with an on-table realization operating at telecom wavelengths. To verify its feasibility for extension over a long distance, we have furthermore reported an illustration on a 1 km fiber. In both cases, high visibilities of more than 98% are achieved through active stabilization of interferometers. Our demonstration is crucial as a direct verification of such a remarkable application, and this procedure can become a key communication module for revealing fundamental physics through counterfactuals.

DOI: 10.1103/PhysRevLett.109.030501 PACS numbers: 03.67.Dd, 03.67.Hk

The principle of quantum mechanics leads to exciting opportunities across a number of applications offering high performance, superiority, or fundamental new understanding of physics over classical methods. There are many fundamental quantum phenomena that lead to intriguing physical effects [1–6]. Among them, several striking paradigms come in the form of counterfactual phenomena. For example, Elitzur and Vaidman propose interaction-free quantum interrogation of classical objects through the wave-particle duality of light, in which the presence of a nontransmitting object is ascertained seemingly without interacting with it [2], i.e., with no photon absorbed or scattered by the object. Furthermore, the logic underlying the coherent nature of quantum information processing enables counterfactual computation [3], in which the potential outcome of a quantum computation can be inferred, even if the computer is not run. Conditional on the as-yet-unknown outcome of the computation, it is sometimes possible to counterfactually infer information about the solution. Experimental demonstrations have been realized for high-efficiency ''interaction-free'' measurements [4] via the quantum Zeno effect and for counterfactual quantum computation through quantum interrogation [5]. These proposals and experimental realizations constitute a number of surprising effects, coming from counterfactuals in quantum mechanics and revealing many new understandings of fundamental quantum physics.

Recently, an extremely remarkable scheme named ''counterfactual quantum cryptography'' [1] was proposed by Noh for performing key distribution. In order to produce identical secure keys between two remote communication parties, a key distribution process generally requires the actual transmission of signal particles through a quantum channel before detection and data postprocessing. Quantum key distribution (QKD) in fact appears as the first application with provable unconditional security between the communicating parties. Since the proposal of BB84 protocol [7] for quantum key distribution, there has been a flurry of activity in both theoretical development and successful experimental demonstrations of quantum cryptography systems ranging from a two-party communication to a network [7–27]. These proposals and demonstrated protocols, however, require the paradigm of actual ''signal particle transmission.'' However, Noh's proposal, for the first time, offers an approach that allows us to do secret communications using counterfactual quantum phenomena. In this method, quantum signals producing secure final keys are not actually transmitted. The method exploits very interesting physics, making use of a conceptually new approach to perform secure communications. Similar to the route developed for the traditional QKD method, an unconditional security proof is attempted [28] in an ideal case by utilizing a perfect single-photon source with well-controlled detector efficiencies, etc. Although an experimental realization is presented in [29] with a modified scheme, it utilizes a ''plug and play'' type Mach-Zehnder interferometer. The final key is produced from photons that actually travel across Bob's site. Thus, the demonstration is, in fact, not equivalent to the original protocol and faces potential security threats. In fact, a complete and faithful demonstration remains a challenge, whose feasibility is open for even a proof-in-principle realization. The counterfactual method for secure communication provides the distinguishing employment of quantum principles for an applicable task, and would motivate us to a novel conceptual thinking on fundamental quantum physics.

In this Letter, we demonstrate the first faithfully experimental implementation of the counterfactual quantum communication (CQC) scheme, operating at telecom wavelengths. We have developed several key techniques for achieving a complete and robust realization. The most crucial part involved in the scheme is a stabilized interferometer. To maintain favorable conditions for the successful operation of quantum communication, we develop an active feedback control technology for real-time stabilization of the Michelson-type interferometer used in the scheme. Tailored optical and controlling electronics designs are made, allowing us to attain high visibility for the interferometers. A truly analog proportional-integral (PI) circuit is developed for real-time feedback control. We carefully choose the desired optical switch with the one made from $LiNbO_3$, which allows no phase change when switching back. We first set up the experiment with an on-table test. To check the feasibility for long-distance realization, we extended the experiment to a 1 km fiber. In both cases, high visibilities of more than 98% are attained for the interferometers, successfully demonstrating intriguing physics through our experimental verifications.

A schematic of the experimental setup is illustrated in Fig. 1. Two distributed feedback laser diodes (LDs) with pulse width of about 1 ns for generating horizontal and vertical polarizations are combined with a polarization beam splitter (PBS) to act as signal light. The center wavelength of the two LDs were carefully tuned to be consistent within a range of 0.02 nm. To avoid possible side-channel attacks, one should use narrower pulses or a single laser along with beam splitters, polarizing beam splitters, and optical switches before attenuation, which is easily attained technically, as shown in our previous work [26]. A random number will be supplied to Alice to enable her generate a sequence of pulses with random polarization $|H>$ or $|V>$. An attenuator is used to attenuate the pulse to the single photon level at Alice's output port. As depicted by the protocol, the signal pulse is split by a beam splitter (BS), and then it travels through arm a or arm b for transmission. A polarization controller (PC) is inserted for compensating possible polarization drifts of the fiber channel. In the protocol, Bob will randomly choose one of the two polarizations representing his bit value. The optical path b of the single-photon pulse will be blocked if the polarization of the pulse is identical to his polarization. For achieving this, a tailored PBS is used with the reflecting port connected with a jumper, which is about 20 m long, enough for accumulating the time needed to change the status of the optical switch (SW). This design allow us to set a delay for H and V pulses; horizontal light will pass the PBS directly, while vertical light will reflect to the delay line, and then transmit back to another output port of PBS before going through SW. Bob can therefore control the switch timing accurately so as to guide the signal photon to be directly detected by his polarization sensitive detector, or be rotated and reflected by the Faraday rotator mirror (FM) and return back to BS. In our experiment, polarization-sensitive detection is accomplished by a PBS and two single-photon detectors. Therefore, through accurate control of the switch timing, Bob can determine effectively whether to switch the polarization state to the detector $D3$ or not.

If Bob chooses a different polarization from Alice, the pulse will be reflected by Bob and combined again at BS.

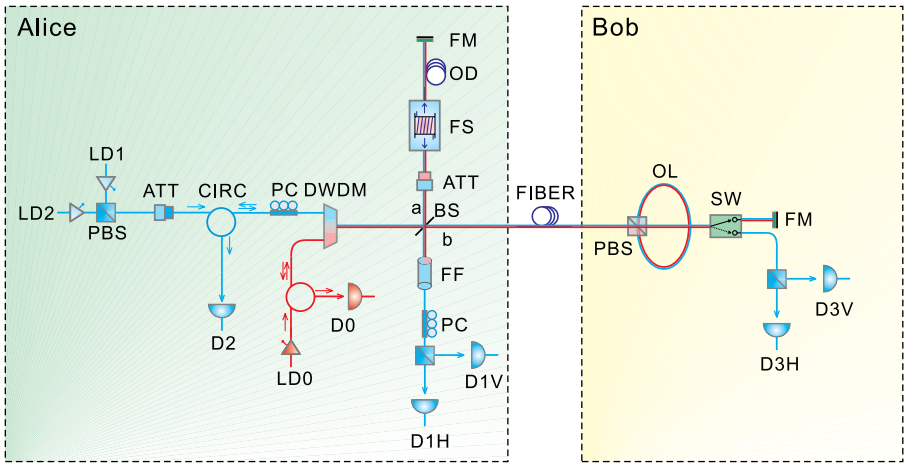

FIG. 1 (color online). Schematic setup of fiber-based counterfactual quantum cryptography system. A signal photonic pulse is sent from Alice's side before it passes through an optical circulator and then is split by a BS to travel along paths a and b. Then, the pulse goes through a Michelson-type interferometer. Sifted keys will be established by selecting only the events for which $D1$ alone detects a photon with a correct final polarization state. LD: laser diode; PBS: polarization beam splitter; ATT: fiber attenuator; CIRC: optical circulator; PC: polarization controller; BS: beam splitter; FS: fiber stretcher; DWDM: dense wavelength division multiplexer; FF: fiber filter; OD: optical delay line; OL: optical loop; SW: fiber switch; FM: Faraday rotator mirror; $D0$, $D1$, $D2$, $D3$: detectors; $D1H$ and $D1V$ are short notions of detector $D1$ for detecting horizontal and vertical polarization, the same for $D3H$ and $D3V$.

In this case, the photonic pulse will go toward detector $D2$ because of interference effect if there is a phase difference of π radians between the two paths a and b. An attenuator is added to arm a to balance the optical loss between the two arms. To compensate the phase drift in the fiber and be sure that all the light after interference will go to detector $D2$, a fast fiber stretcher (FS) is used for compensating fast phase variation in the two arms. Furthermore, Alice employs an optical delay (OD) line to adjust the path difference between arm a and arm b of the whole system with a precision of less than 0.1 mm. In order to obtain good visibility in the interferometer, feedback control is further developed by using a laser with a different wavelength of 1570 nm and controlling electronics. The feedback laser and the signal laser are combined by a dense wavelength division multiplexer (DWDM) before entering the BS.

If the choices of Bob and Alice are the same, the interferometer will be destroyed, since Bob chooses to detect rather than let it go through, and either Alice's $D1$ or $D2$ or Bob's $D3$ will detect a pulse signal. We save only events for $D1$ clicks, and keep all other events for monitoring Eve's intervention. For $D1$'s clicks, only the events for which $D1$ detects a correct final polarization will be kept by Alice and no information is revealed, and otherwise the measurements results are announced. For $D2$ or $D3$'s clicks, both the detected and initial polarization states are released for detection of possible eavesdropping. According to the scheme, the initial quantum state after the BS can be rephrased as one of the following two orthogonal states: $|\phi_0\rangle = \sqrt{T}|0\rangle_a |H\rangle_b + i\sqrt{R}|H\rangle_a |0\rangle_b$ and $|\phi_1\rangle = \sqrt{T}|0\rangle_a |V\rangle_b + i\sqrt{R}|V\rangle_a |0\rangle_b$. Here, R and T are the reflectivity and transmissivity rates, respectively, of the BS. In our case, R and T are 50%/50%. The variables a and b denote the path toward Alice's Faraday rotator mirror and Bob's site, respectively. We use $|0\rangle_a$ and $|0\rangle_b$ to represent the vacuum states in the modes a and b, respectively. As for the events for which $D1$ detects a correct final polarization, the initial state will collapse into two states of $|H\rangle_a|0\rangle_b$ or $|V\rangle_a|0\rangle_b$. In fact, Bob will extract the secure keys with Alice from nondetection events.

In the experiment, we use a 1550-nm distributed feedback (DFB) laser as the signal source that is actively modulated into about 1 ns pulse width. The intensity of the laser was attenuated to 0.1–1 photon/pulse on average at the output of Alice's side. The total loss of arm b was measured to be around 10.5 dB when the photon goes through and returns back after Bob's FM for the case of an on-table test. The system works at a repetition rate of 100 kHz. Currently, this is mainly limited by the performance of feedback loop. In addition, the response time of the fiber switch of about 100 ns and the switching time of about 300 ns are needed to choose the polarization of each pulse.

An active feedback control system is developed for phase stabilization. Using a DWDM, we couple the signal light and the 1570-nm reference light of a DFB cw laser before they enter the BS. When the system works in feedback mode, Bob always decides to reflect the reference light by choosing the optical switch to the FM. The reference light goes through the interferometer via the same path of the signal light and goes back through the DWDM to a different optical circulator output. A highly sensitive avalanche photodiode (APD) D0 is used to detect the intensity of the interferometer output. Thus, the reference light goes through the same interferometer as the signal light and experiences the same path difference. However the phase differences are different on account of the different wavelengths of the signal and reference lights. Following a similar analysis shown in [30], we illustrate the phase difference with $n \triangle L = \lambda_r(m_r + \varphi_r/2\pi) = \lambda_s(m_s + \varphi_s/2\pi)$. Here, n is the refractive index, and the subscripts r and s refer to the reference and signal lights, respectively. $\triangle L$ is the path difference. The relative phase difference φ_r, φ_s has a relation with its wavelength λ for a fixed setup. The variable m is an integer, indicating phase difference being an integral multiple of its wavelength. The intensity of the interferometer output can be given by $I = I_0\cos^2(\frac{k\triangle L}{2})$ where k gives the wave number. By stabilizing the reference output intensity to a settled level, one can fix the path difference for the signal light. A homemade PI controller from a cold-atom experiment is modified and adjusted for our experimental need. A voltage amplifier is used to control the fiber stretcher, which can quickly change the relative length of the fiber in path a. The PI controller compares the APD output with a preset monitor level. If the APD output voltage differs from the monitor level, the PI circuit will adjust the output voltage for compensating the change. For our 1 km system, phase change is roughly in a level of 0.1–0.5 rad/ms. A total range of 20 V(-10 V + 10 V) output with a subsequent amplification factor of 10–40 times enables us to make a 200π rad adjustment through fiber stretcher. A final interference visibility of more than 98% is observed for both the desktop test and the 1 km fiber cable application cases, enabling the successful operation of the feedback controlling system. Continuous running of about an hour for the desktop test and 900 s for the 1 km application case have shown stable and reliable performances.

A field-programmable gate array (FPGA) electronics board is developed for controlling the signal laser, detectors, and fiber switch. The timing is about 1 μs for signal pulse generation and detection and 9 μs feedback time for the PI circuit within a 10 μs duty circle for FPGA. We use one 1570-nm DFB laser as reference light. We first implemented the scheme in the on-table test case. With PI feedback, a fringe visibility of more than 98% could be maintained. A raw key of 185651 bits is generated within a 3617 s running (amounting to 51.3 bits/s), with an average quantum bit error rate (QBER) of 6.8% when the average photon number is 0.5 photon/pulse. If we change the

average photon number to 0.05 photon/pulse, the raw key of 7891 bits will be produced with a QBER of 4.2% on average. To test the feasibility of CQC, we extended the scheme to a 1 km fiber cable connecting the sites of Alice and Bob, which will cause a channel loss of about 1 dB. A fringe visibility of about 98% is managed to be attained for a 1 km fiber as well, which allows the generation of secure keys. Without any cover for fibers on the experimental desktop, a raw key of about 126 bits/s is obtained with the QBER of about 5.8% for 900 s continuous running, when the average photon number is chosen to be 1.0 photon/pulse. If the average photon number is reduced to 0.5 photon/pulse, the measured QBER is about 5.5%, while the raw keys is decreased to around 94 bits/s due to longer feedback time. See Table I for performance details. We see that for the 1 km fiber realization, one can obtain considerable raw key rates of 126 bits/s and good performance, with a rather low error rate of 0.6% through $D3$ for channel monitoring when using an average photon number of 1.0.

To have a more comprehensive understanding of the running of the experiment, we present a circumstantial analysis of the experiment's imperfections. Suppose we have two groups of data, one in which Alice and Bob choose the same random numbers, and the other in which they choose different random numbers. The group with the same number will create a raw key when $D1$ is detected with a correct basis fulfilled with the polarization not disturbed. The other group will create a possible wrong key when $D1$ is detected with a correct basis that contributes to an error. Here, we take the case of the 1 km experiment with a mean photon number of 0.5 for an example to analyze. We attribute all the errors mainly to three parts. The first part is from dark counts and after pulses of the detectors. The detectors we used have a dark count possibility for each gate of about 10^{-5}. With a 100-kHz working frequency, about 1 dark count is created by detector, which will therefore contribute to an error rate of about 0.7%, as the total counts of $D1$ comes to about 70 counts per second in this case. The after pulse will lead to an error rate of about 0.5% due to an after-pulse probability of 1% for detectors. The second part is from the fiber switch's finite extinct ratio. We tested the static extinction ratio of the fiber switch and found it to be 20 dB, with a slightly lower ratio of about 17 dB with regard to the dynamic extinction ratio, which amounts to an error rate of approximately 1%–2%. The third one comes from imperfection of the optical alignment and finite visibility of the feedback system, which will still lead to clicks for $D1$ even if Alice and Bob have different choices. When Alice and Bob choose different random numbers, a visibility like 98% is supposed to be achieved. This means that 1% of the pulses are detected by $D1$ and the other 99% by $D2$. The error rate can thus be estimated to be $0.01/(0.01 + 0.25) = 3.8\%$, by considering the fact that only $1/4$ of the total pulses will be detected by $D1$ when Alice and Bob choose the same random number. All three parts would therefore lead to a QBER of around 6%, as confirmed by actual measured experimental data.

TABLE I. Experimental performance under desktop and 1 km fiber tests. We summarize here the various measured parameters characterizing performances for the desktop and 1 km fiber cases under different average photon numbers. Besides the symbols introduced in the main text, here we use "Total counts" to denote the sum of all the detectors, $D1$, $D2$, and $D3$. "$D2$ same" and "$D2$ diff." refer to the counting of $D2$ when Alice and Bob choose the same bit values and different values, respectively. "Multiple" means all the counts for events of which there are at lease two detector clicks. APN: average photon number; R: raw key (bits).

Platform	APN	R	QBER	Total counts	Time (s)
Desktop	0.5	185 651	6.8%	4 891 623	3617
Desktop	0.05	7891	4.2%	151 626	627
1 km fiber	1.0	113 762	5.8%	1 948 287	900
1 km fiber	0.5	11 278	5.5%	191 347	158
Platform	$D2$ same	$D2$ diff.	$D3$ same	$D3$ diff.	Multiple
Desktop	231 482	1 060 186	3 272 114	23 673	8758
Desktop	9440	28 386	103 228	319	38
1 km fiber	75 628	497 549	1 216 859	7210	6376
1 km fiber	7520	49 224	118 318	487	362

A preliminary security analysis is given in [1] showing a new type of noncloning principle for orthogonal states: if reduced density matrices of an available subsystem are nonorthogonal and the other subsystem is not allowed access, it is impossible to distinguish two orthogonal quantum states $|\phi_0>$ and $|\phi_1>$ without disturbing them. Moreover, the scheme is robust to the so-called photon-number splitting attack. Since Eve cannot access the nondetection process that extracts the secret keys [1], these distinctive properties provide a security advantage over existing schemes. Consider a typical noise channel case as analyzed in [28] in which a possible upper bound for phase error rate could be less than QBER; our system allows sufficiently to generate secure keys after a one-way key distillation process [9] for an ideal case of source and detectors.

We have achieved a faithful and complete realization of counterfactual quantum communication, in which information carriers have seemingly not traveled in the quantum channel. From the desktop test to the setup with a 1 km fiber cable, we have given the first proof-in-principle demonstration of CQC. This confirms the feasibility of CQC, and one can infer that the mere possibility for signal particles to be transmitted is sufficient to create a secret key. We may remark that, to ensure such a possibility, partial signal particles still need to travel randomly along the quantum channel for detection of possible eavesdropping. Such an implementation by exploiting counterfactual effects has revealed new surprising physics behind

quantum mechanics, in addition to the existing experimental demonstrations of ''interaction-free'' measurements [4] and counterfactual quantum computation [5]. A number of key techniques are developed to achieve a complete and robust realization, particularly the active feedback control technology for maintaining real-time stabilization of Michelson-type interferometers. Tailored optical and controlling electronics designs, and special optical switches are made and chosen as well to attain high visibilities for interferometers. One may be surprised that in the implemented scheme, signals pass through the channel twice and thus suffer losses twice. It should be remarked that the CQC scheme in fact acts like the normal BB84 protocol for the communication of overhead transmission loss if one assists with a quantum repeater through the Duan-Lukin-Cirac-Zoller (DLCZ) scheme [31] to teleport single-photon signals directly between Alice and Bob. Also, one may see that the scheme needs to maintain long-term subwavelength stability of the path difference between the two arms of a long-distance interferometer, which can however be overcome by utilizing state-of-the-art technology, similar to the one developed in [32] for coherent optical phase transfer over a 30 km fiber. It is worthwhile to point out here that by using a weak coherent source in place of a true single-photon source, the present demonstration is robust against the normal ''intercept and resend'' attack and ''photon number-splitting'' attack, as analyzed in [1]. A realization employing a triggering single-photon source is within reach by using sources that are produced from spontaneous parametric down-conversion processes or quantum dots, etc. We can see that our implementation is based on currently available technologies, promising a conceptually novel quantum communication system compared with existing systems. Presently, the performance of our system is mainly limited by the speed of feedback. Note that our feedback system is a modification of the PI used in our cold-atom experiments. Significant improvements can be made by combining the method developed in [30] for interferometer stabilization and employing tailored designs with a differential circuit, an autoreset function, and by exploiting an adjacent channel in the C band of 1550.12 nm. Although technically challenging, our implementation in conjunction with the optimizing quality of interference via improved optical design appears to be a viable route toward extendable realization for long-distance fibers.

Y. L. and L. J. contributed equally to this work. We acknowledge the financial support from the CAS, the National Fundamental Research Program of China under Grant No. 2011CB921300, the National High Technology Research and Development Program (863 Program) of China under Grant No. 2009AA01A349, the NNSFC, and the Fundamental Research Funds for the Central Universities. The authors are grateful for the valuable discussions with Professor Xiang-Bin Wang and Dr. Xian-Min Jin.

*kaichen@ustc.edu.cn
†tychen@ustc.edu.cn

[1] T. G. Noh, Phys. Rev. Lett. **103**, 230501 (2009).
[2] A. C. Elitzur and L. Vaidman, Found. Phys. **23**, 987 (1993).
[3] G. Mitchison and R. Jozsa, Proc. R. Soc. A **457**, 1175 (2001).
[4] P. G. Kwiat, A. G. White, J. R. Mitchell, O. Nairz, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **83**, 4725 (1999).
[5] O. Hosten, M. T. Rakher, J. T. Barreiro, N. A. Peters, and P. G. Kwiat, Nature (London) **439**, 949 (2006).
[6] V. Parigi, A. Zavatta, M. S. Kim, and M. Bellini, Science **317**, 1890 (2007).
[7] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), pp. 175–179.
[8] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[9] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[11] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[12] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).
[13] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[14] H.-K. Lo, X.-F. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[15] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, Proc. SPIE Int. Soc. Opt. Eng. **5815**, 138 2005.
[16] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[17] Y. Zhao, B. Qi, X.-F. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
[18] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).
[19] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).
[20] T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).
[21] Z.-L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).
[22] M. Peev *et al.*, New J. Phys. **11**, 075001 (2009).
[23] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[24] Q. Zhang *et al.*, New J. Phys. **11**, 045010 (2009).
[25] W. Chen *et al.*, IEEE Photonics Technol. Lett. **21**, 575 (2009).
[26] T.-Y. Chen *et al.*, Opt. Express **18**, 27217 (2010).
[27] M. Sasaki *et al.*, Opt. Express **19**, 10387 (2011).
[28] Z.-Q. Yin, H.-W. Li, W. Chen, Z.-F. Han, and G.-C. Guo, Phys. Rev. A **82**, 042335 (2010).
[29] M. Ren, G. Wu, E. Wu, and H. Zeng, Laser Phys. **21**, 755 (2011).
[30] S.-B. Cho and T.-G. Noh, Opt. Express **17**, 19027 (2009).
[31] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature (London) **414**, 413 (2001).
[32] S. M. Foreman, A. D. Ludlow, M. H. G. de Miranda, J. E. Stalnaker, S. A. Diddams, and J. Ye, Phys. Rev. Lett. **99**, 153601 (2007).